RESEARCH AND APPLICATION OF THE LAW TO CYBER INCIDENTS
Introduction

Cameron Brown
MInsSt, MPict
LL.B, B.A (Behavioural Science)
Grad.Cert (Computer Crime Investigation)

+49 (0) 151 674 50404

Experience

Legal Practice
Law Enforcement
Policing
Government
United Nations
Transparency International

Academic Institutions: ANU, Oxford, Max Planck

Industry / Commerce: Attorney, Forensic Investigator, InfoSec Professional and Trusted Advisor (Ernst & Young)

- Cyber Crime Defence Advisor
- Information Security Strategist
- International Legal Practitioner
- Published Author
The views and opinions expressed in this presentation are solely those of the presenter and do not represent any official policy or position of past or present employers of the presenter.

The material in the following slides is for informational purposes only and should in no way be construed as advice of any kind.
Criminal and civil cases involving electronic evidence

<table>
<thead>
<tr>
<th>Civil Investigations</th>
<th>Criminal Investigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access to information systems</td>
<td>Fraud</td>
</tr>
<tr>
<td>Unauthorized data duplication</td>
<td>Insider trading</td>
</tr>
<tr>
<td>Industrial espionage</td>
<td>Possession of prohibited material</td>
</tr>
<tr>
<td>Termination of employment</td>
<td>Theft of intellectual property and trade secrets</td>
</tr>
<tr>
<td>Breach of contract</td>
<td>Stalking and threatening behavior</td>
</tr>
<tr>
<td>Breach of corporate policy</td>
<td>Sabotage of information systems</td>
</tr>
<tr>
<td>Harassment in the workplace</td>
<td>Theft of property and assets</td>
</tr>
<tr>
<td>Bankruptcy and insolvency</td>
<td>Counterfeit and forgery</td>
</tr>
<tr>
<td>Due diligence inquiries</td>
<td>Assault and sexual offences</td>
</tr>
<tr>
<td>Loss of inventory</td>
<td>Homicide</td>
</tr>
<tr>
<td>Disclosure of personally identifiable information</td>
<td>Drug trafficking</td>
</tr>
<tr>
<td>Negligence</td>
<td>Money laundering</td>
</tr>
</tbody>
</table>

Source: Brown
## Principles of criminal jurisdiction

| Principle of territoriality (Objective territorial principle) | A state can prosecute activities upon its territory, even in cases where an offender is a foreign citizen.  
If the perpetrator is outside of the territory, territorial jurisdiction nonetheless includes where one of the constituent elements of the offence, and more especially its effects, take place within the territory. The objective territoriality principle thus ensures that both the state where the behaviour commenced, and the state where the offence was concluded may validly try the alleged perpetrator. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Effects Doctrine</td>
<td>Jurisdiction is established over foreign conduct that produces substantial effects within the territory.</td>
</tr>
</tbody>
</table>
| Principle of nationality (Active) | Jurisdiction is established depending upon the nationality of the individual concerned.  
Jurisdiction is established based on the nationality of the offender, wherever the crime is committed.  
Jurisdiction is established based on the nationality of the victim, wherever the crime is committed. |
| Habitual residence | Jurisdiction is established based on the place of habitual residence of the offender. |
| Protective principle | Jurisdiction is established where a criminal act abroad is derogatory to the security of the state concerned and/or touches upon its vital interests. |
| Principle of universality | Jurisdiction is established over any person accused of committing a small number of 'international crimes,' such as piracy, war crimes and grave breaches of the Geneva Conventions, regardless of the territory or the nationality of individuals involved. The principle is usually limited to situations where the state with territorial jurisdiction is unable or unwilling to prosecute. |

Source: UNODC
Application of the law to cybercrime investigation

Source: UNODC
Economic Community of West African States legal approach

- Criminalization
- Procedures
- Electronic evidence
- Jurisdiction
- Service Provider Liability
- International Cooperation

ECOWAS Directive on Cybercrime
Council of Europe legal approach

- Criminalization
- Procedures
- Jurisdiction
- International Cooperation
- Electronic evidence
- Service Provider Liability
- International Cooperation

Council of Europe Convention on Cybercrime
Commonwealth legal approach

Criminalization

Procedures

Electronic evidence

Jurisdiction

Service Provider Liability

International Cooperation

Commonwealth Model Legislation

@AnalyticalCyber

cameron.brown@legalforensic.com

CAMERON BROWN - Research and application of the law to cyber incidents
## Instruments related to cyber incidents

<table>
<thead>
<tr>
<th>BINDING</th>
<th>NON-BINDING</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (2007)</td>
<td></td>
</tr>
<tr>
<td>• Commonwealth of Independent States (CIS) Agreement on Cooperation in Combating Offences related to Computer Information (2001)</td>
<td></td>
</tr>
<tr>
<td>• Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security (2009)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• International Telecommunication Union (ITU)/Secretariat of the Pacific Community Model Law on Cybercrime (2011)</td>
</tr>
</tbody>
</table>

Source: UNODC
UN Comprehensive study on cybercrime

UNODC Response

UNODC promotes long-term and sustainable capacity building in the fight against cybercrime through supporting national structures and action. Specifically, UNODC draws upon its specialized expertise on criminal justice systems response to provide technical assistance in capacity building, prevention and awareness raising, international cooperation, and data collection, research and analysis on cybercrime.

- Global Programme on Cybercrime
- Comprehensive Study on Cybercrime - Arabic - Chinese - English - French - Russian - Spanish

The translation of the Comprehensive Study on Cybercrime was facilitated by the extrabudgetary contribution of the Chinese Government.

Source: UNODC

TRANSLATION LINKS

Spanish:
https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

Arabic:
https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Arabic.pdf

Chinese:

English:

French:

Russian:
https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf
Legal systems participating in the study

Source: UNODC
### Focal points for existing and developing cybercrime legislation

<table>
<thead>
<tr>
<th>Area</th>
<th>Existing legislation</th>
<th>New or planned legislation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminalization</td>
<td>27%</td>
<td>38%</td>
</tr>
<tr>
<td>Investigative measures</td>
<td>15%</td>
<td>17%</td>
</tr>
<tr>
<td>Jurisdiction</td>
<td>11%</td>
<td>14%</td>
</tr>
<tr>
<td>Electronic evidence</td>
<td>9%</td>
<td>13%</td>
</tr>
<tr>
<td>International cooperation</td>
<td>6%</td>
<td>12%</td>
</tr>
<tr>
<td>Prevention</td>
<td>6%</td>
<td>9%</td>
</tr>
<tr>
<td>Public-private cooperation</td>
<td>5%</td>
<td>5%</td>
</tr>
<tr>
<td>Other</td>
<td>6%</td>
<td>5%</td>
</tr>
</tbody>
</table>

Source: Study cybercrime questionnaire. Q12 and Q14. (n=55,36; r=262,111)

Source: UNODC
Structure of international and regional instruments

Source: UNODC
Instruments for drafting or developing national cybercrime legislation

<table>
<thead>
<tr>
<th>Instrument</th>
<th>Existing Legislation</th>
<th>New or Planned Legislation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Council of Europe Convention on Cybercrime (2001)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>European Union instruments</td>
<td>46%</td>
<td>52%</td>
</tr>
<tr>
<td>Council of Europe Convention on the Protection of Children (2007)</td>
<td>4%</td>
<td>16%</td>
</tr>
<tr>
<td>Additional Protocol to Council of Europe Convention on Cybercrime (2003)</td>
<td>15%</td>
<td>12%</td>
</tr>
<tr>
<td>Other Legislation</td>
<td>15%</td>
<td>12%</td>
</tr>
<tr>
<td>Arab League Model Law (2004) or Arab Convention (2010)</td>
<td>8%</td>
<td>12%</td>
</tr>
<tr>
<td>Ecowas Draft Directive on Cybercrime (2009)</td>
<td>8%</td>
<td>12%</td>
</tr>
<tr>
<td>National legislative models</td>
<td>8%</td>
<td>15%</td>
</tr>
<tr>
<td>CIS Cooperation Agreement (2001)</td>
<td></td>
<td>4%</td>
</tr>
</tbody>
</table>

Source: Study cybercrime questionnaire. Q12 and Q14. (n=26.25; r=51, 50)

Source: UNODC
Cybercrime acts involving a transnational dimension

Source: UNODC
## Types of informal cooperation among LEAs

<table>
<thead>
<tr>
<th>Forms of informal cooperation</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>General technical advice</td>
<td>42%</td>
</tr>
<tr>
<td>General legal advice</td>
<td>39%</td>
</tr>
<tr>
<td>Identity or subscriber information for a suspect</td>
<td>35%</td>
</tr>
<tr>
<td>Conduct of a joint investigation</td>
<td>35%</td>
</tr>
<tr>
<td>Expedited preservation of computer data</td>
<td>23%</td>
</tr>
<tr>
<td>Other (unspecified)</td>
<td>10%</td>
</tr>
<tr>
<td>Provisional arrest of a suspect</td>
<td>3%</td>
</tr>
<tr>
<td>Search for computer hardware or data</td>
<td>3%</td>
</tr>
<tr>
<td>Seizure of computer hardware or data</td>
<td>3%</td>
</tr>
<tr>
<td>Stored traffic data from a service provider</td>
<td>3%</td>
</tr>
</tbody>
</table>

Source: Study cybercrime questionnaire. Q106. (n=31, r=61)

Source: UNODC
# Cooperation provisions in cybercrime instruments

<table>
<thead>
<tr>
<th>International cooperation provisions</th>
<th>Binding instruments</th>
<th>Non-binding instruments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft African Union Convention</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Commonwealth of Independent States Agreement</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Council of Europe Cybercrime Convention</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>League of Arab States Convention</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>World Intellectual Property Organization Convention</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Model Bill</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Commonwealth Model Law</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>ITU/ICANN/ECTL Model Legislative Texts</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

| General international cooperation | ✔ | ✔ |
| Extradition for instrument offences | ✔ | ✔ |
| General mutual legal assistance | ✔ | ✔ |

| Specific assistance | ✔ | ✔ |
| Preservation of computer data | ✔ | ✔ |
| Seizure/access to/collection of/disclosure of computer data | ✔ | ✔ |

| Other forms of cooperation | ✔ | ✔ |
| Transit/border access | ✔ | ✔ |
| 24/7 network | ✔ | ✔ |
| Additional provisions | ✔ | ✔ |
| Dual criminality requirements | ✔ | ✔ |

Source: UNODC
Avenues for obtaining extra-territorial assistance

Source: Study cybercrime questionnaire. Q105. (n=56, r=221)

Source: UNODC
Permissibility of trans-border data access by foreign LEA

Source: UNODC

Source: Study cybercrime questionnaire. Q108. (n=47)
Practical and legal means to obtain information from service providers

Source: Cybercrime study questionnaire. Q102. (n=58)

Source: UNODC
## Service providers and available data types

<table>
<thead>
<tr>
<th>Subscriber Data</th>
<th>Traffic/Transactional Data</th>
<th>Content Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and address</td>
<td>Connection logs detailing dynamic or static IP addresses assigned by the service provider and Uniform Resource Locators (URLs)</td>
<td>Stored electronic communications retrieved from remote computing services (e.g., email messages, SMS/MMS messages, pages messages, voice mail, video messages)</td>
</tr>
<tr>
<td>IP address used to register an account</td>
<td>Account usage logs reflecting IP addresses accessed via a subscription service</td>
<td>Stored electronic communications from remote computing services not yet retrieved (e.g., stored fax messages, synchronized data associated with cross-platform applications)</td>
</tr>
<tr>
<td>Telephone number</td>
<td>Information exchanges processed through a service provider (e.g., email header information, records of shared folders)</td>
<td>Records of financial transactions stored in online banking accounts and payment facilities (e.g., PayPal) including records of transfers using digital currencies (e.g., Bitcoin wallets)</td>
</tr>
<tr>
<td>Email address</td>
<td>Records of wireless carrier services pointing to the location of a subscriber’s device (e.g., triangulation of cell tower data, GPS coordinates)</td>
<td>Data uploaded, downloaded or shared via cloud services (i.e., platform as a service, infrastructure as a service, software as a service, network as a service)</td>
</tr>
<tr>
<td>Credit card particulars, direct debit account details, or other method of payment</td>
<td>Itemized records logging usage (e.g., numbers dialed, time and date of calls, communication logs)</td>
<td>Managed and automated backup services for computers and mobile devices (e.g., iCloud, OneDrive)</td>
</tr>
<tr>
<td>Service agreement information (e.g., commencement date)</td>
<td>Information identifying the sender and recipient, including copy recipients, for a communication (e.g., email header information, shared folders, attachments)</td>
<td>Data hosted in datacenters and cloud computing environments (i.e., private, community, public clouds, hybrid clouds)</td>
</tr>
<tr>
<td>Geographical location of a service</td>
<td>Routing information identifying equipment through which a communication is, or has been transmitted (e.g., dynamic IP address allocation, file transfer logs)</td>
<td>User data associated with social networking platforms (e.g., screen names, contact lists, multimedia, documents, messages, postings)</td>
</tr>
<tr>
<td>Internet connection records (e.g., quantity of data downloaded and/or uploaded)</td>
<td>Time and duration of service usage (e.g., session times, calls and/or connections)</td>
<td>Use of subscription-based telecommunications services (e.g., conference calling, call messaging, call waiting, call barring, call forwarding, call redirection, calling line identification services)</td>
</tr>
<tr>
<td>Use of subscription-based telecommunications services (e.g., conference calling, call messaging, call waiting, call barring, call forwarding, call redirection, calling line identification services)</td>
<td>Use or selection of preferential numbers or discount calls</td>
<td>Service providers and available data types</td>
</tr>
<tr>
<td>Use of subscription-based telecommunications services (e.g., conference calling, call messaging, call waiting, call barring, call forwarding, call redirection, calling line identification services)</td>
<td>Connection, disconnection and reconnection of services</td>
<td>Source: Brown</td>
</tr>
<tr>
<td>Use or selection of preferential numbers or discount calls</td>
<td>Addresses or other markings written on, or associated with, a postal item (e.g., names, telephone numbers, tracking numbers)</td>
<td>Source: Brown</td>
</tr>
</tbody>
</table>

Source: Brown
Cybercrime investigation training for non-specialized judges

Source: Study cybercrime questionnaire. Q192. (n=32)

Source: UNODC
Stakeholders and incentives

- Criminals
- Industrial competitors
- Foreign intelligence
- Common users and insiders
- State sponsored actors
- Hackers
- Non-state actors

Different stakeholders and their incentives
Criminals

► Making money through fraud or from the sale of valuable information

► Realising gains on the stock market by obtaining information prior to announcement of official transactions

► Extorting money from private entities by holding data to ransom or interfering with online transactions of a commercial nature

► Indulging in depravity by disseminating abusive material and satisfying predatory urges
Industrial competitors

- Stealing intellectual property and trade secrets
- Gaining advantage in the marketplace by acquiring commercially sensitive data, such as key negotiating positions
- Furthering privatisation strategies by discrediting counterparties to a transaction
- Undermining market value of a target to manipulate favorable terms of procurement
State sponsored actors

- Advancing homeland security through ubiquitous surveillance
- Collaborating with likeminded nation-states to solve shared problems
- Monitoring political speech online and silencing dissidents
- Sabotaging international deals to safeguard and enhance domestic commercial interests, or give local industries an economic advantage
- Undermining credibility of enemies of the state (trolling)
Non-state actors

- Disrupting government services and obstructing capacity of industry to function
- Exploiting information security weaknesses to raise awareness, exact revenge or expose wrongdoing
- Attacking critical infrastructure for political or ideological reasons
- Circulating graphic material to traumatize adversaries and defacing digital resources to further a political agenda
Common users and insiders

- Accidental or deliberate system misuse by users who have legitimate access or escalated privileges
- Punishing an employer for perceived grievances
- Monitoring or stalking a significant other
- Planting malicious insiders within an organisation to steal sensitive information
- Harvesting trade secrets for career advancement with a competitor
Highly organised and persistent

Support for operations run by cyber-criminals has evolved into a global enterprise encompassing managed software deployments and scheduled updates, roadmaps for platform development, and even helpdesks to service needs of clients and users. They are innovative and agile illicit businesses which harness the expertise of specialists across various domains of online criminality.
The Nuclear operation accumulated revenue of $100,000 a month. Attackers would rent a Nuclear server with a control panel from which to view and manage a malware campaign. Attackers could disseminate any malware, but the system would not target endpoints in Azerbaijan, Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Uzbekistan and Ukraine (Eastern Partnership). The developer may have resided within one of these jurisdictions and keen to avoid extradition. Ransomware was the dominant payload. Success of attacks leveraging Nuclear measured at 9.95%.
OPSEC for online criminality

- Just as threat perpetrator motivations and capabilities vary from group to group, so does OPSEC tradecraft

- Different actors have different requirements for privacy and anonymity

- For instance, cyber crime forum operators must balance need to stay off the radar of law enforcement with need to sell and market their products
Redefining OPSEC objectives for cybercriminals

- Detect
- Identify
- Observe
- Analyse
- Report

- Disrupt
- Contain
- Minimise
OPSEC: Research and technical development

- Credential harvesting and target profiling
- Uncovering zero-day vulnerabilities
- Exploring new technologies to leverage and exploit
- Developing botnets and malware
- Scanning systems for items of value to sell or exploit
- Following media, blogs and forums to harvest open intelligence and react to activities of LEA

@AnalyticalCyber
OPSEC: BulletProof hosting

Source: Digital Shadows
OPSEC: Precautions

---[ 2 ]--- Staying Safe

This is illegal, so you'll need to take some basic precautions:

1) Make a hidden encrypted volume with TrueCrypt 7.1a [0]
2) Inside the encrypted volume install Whonix [1]
3) (Optional) While just having everything go over Tor thanks to Whonix is probably sufficient, it's better to not use an internet connection connected to your name or address. A cantenna, aircrack, and reaver can come in handy here.

[0] https://truecrypt.ch/downloads/

As long as you follow common sense like never do anything hacking related outside of Whonix, never do any of your normal computer usage inside Whonix, never mention any information about your real life when talking with other hackers, and never brag about your illegal hacking exploits to friends in real life, then you can pretty much do whatever you want with no fear of being v.&.

NOTE: I DO NOT recommend actually hacking directly over Tor. While Tor is usable for some things like web browsing, when it comes to using hacking tools like nmap, sqlmap, and nikto that are making thousands of requests, they will run very slowly over Tor. Not to mention that you'll want a public IP address to receive connect back shells. I recommend using servers you've hacked or a VPS paid with bitcoin to hack from. That way only the low bandwidth text interface between you and the server is over Tor. All the commands you're running will have a nice fast connection to your target.
OPSEC: Mentoring

Alpraking's OPSEC guide to being a successful kingpin.

1. So you want to ship hundreds of thousand of pills a week for years and stay safe?

2. Here's a couple of tips to keep you safe. I've been here since SR 1.8 under various aliases and have, over the course of my 3 years online career, shipped over 10 million pills. I used to press pills myself. Now last time I've seen a press was a year ago. I'm basically just smoking bowls and trolling on Reddit now.

3.

4. 1. Outsource

5. Outsourcing simply refers to the noble art of hiring other people, “pawns of the checker”, to do the dirty work. You want to hire clean people that don't arise suspicions. They will be doing the dirty work so you want to hire someone who isn’t already involved in drug trade or has priors. Don't get me wrong, you’ll do everything in your power to protect them. Remember, if your guys catch heat, it can propagate to deeper layers fairly quickly and ultimately, to you.

6.

7. 2. Separate Administration & Execution

8. Have a layer of people who are doing the "boss" work and another one who is doing the "executive" work. Boss work is mainly paperwork and verifications to ensure everyone is doing his job properly and numbers balance and quality control is in check. Administrators don't get their hands dirty as that they will not handle the drugs themselves, but they will make sure packs are being shipped, tracking codes are being handled, productions are being made correctly and such. Administration is a promotion for executives who have shown a great degree of skill and loyalty. You can’t put just anyone to overlook someone else’s work. You have to get someone who has done it before and will be able to train new personnel or solve irregular issues. I normally promote my executors to administrators once they have shown that they can handle any issue from their business. I have them hire one of their friends and pay both from my own pocket. Employees kind of like hearing "hey, how about you keep your salary, train your friend to do your job, and you both will earn the same thing, paid from the big boss’ pocket." More than money, people want power. Give power to people who want power and keep the money for yourself.

Source: Digital Shadows
Criminal justice system attribution in cybercrime cases

Source: Cybercrime study questionnaire. Q54-70.

Source: UNODC
Evasive criminal techniques

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dead dropping</td>
</tr>
<tr>
<td>2</td>
<td>Cryptography</td>
</tr>
<tr>
<td>3</td>
<td>Use of codes / aliases for communication</td>
</tr>
<tr>
<td>4</td>
<td>Steganography</td>
</tr>
<tr>
<td>5</td>
<td>Compromised intermediaries</td>
</tr>
<tr>
<td>6</td>
<td>Spoofing</td>
</tr>
<tr>
<td>7</td>
<td>Hiding in safe jurisdictions</td>
</tr>
<tr>
<td>8</td>
<td>Anonymity networks and proxy services</td>
</tr>
</tbody>
</table>

“The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you - and then periodically erasing your footprints” (Tor)
A variety of techniques can be employed to enhance anonymity and disguise the perpetrator behind a cyber-attack.

Seasoned attackers move laterally between countries with ‘friendly’ jurisdictions and strategically traverse proxy servers or compromised systems to conceal their identity.

“…we’re living in a world where we can’t easily tell the difference between a couple of guys in a basement apartment and the North Korean government with an estimated $10 billion military budget” (Bruce Schneider)
19 – 20 May 2016 The Hague (NL)

PRIVACY IN THE DIGITAL AGE OF ENCRYPTION AND ANONYMITY ONLINE
Effectively tackling encryption and online anonymity

THE PATH FORWARD – EXAMINING THE CHALLENGES AND OPPORTUNITIES

BALANCING PRIVACY AND SECURITY WITH PROPORTIONALITY:
• Tension between privacy, safety, and police mandates
• “Surrender a little privacy if you want more security” – to what extent can we give up one without undermining the other? Commercial entities championing consumer security - a business model concern and global public brand marketing strategy?

TECHNOLOGY AS AN INHIBITOR AND FACILITATOR
• Security-by-default
• Synchronized lifestyles – cloud and distributed data
• The ‘whack-a-mole’ phenomenon with miscreants and extremists
• Throttling encryption and the ‘weakest link’ phenomenon at the international level
• Quantum computing, brute force, and open source software tools

THE JUDICIARY, LAW ENFORCEMENT, INTELLIGENCE AND PRIVATE ENTITIES
• Human intelligence, the Golden Age of Surveillance, and open sources of intelligence
• Technical interrogation and complimentary role of face-to-face engagement with suspects
• Sophisticated adversaries and deniability – a technical and legal challenge
• Mandatory disclosure and the key role of the judiciary – judgment-in-default
• Compelling individuals and organisations to disclose decryption keys
• Law as a punitive measure and persuasive mechanism
• Legislators should be mindful of avoiding ‘sui generis’ modalities - tailoring laws to meet changes in technology
• Lawful surveillance orders must meet the requirements of human rights and the rule of law
Digital idealism
Digital realism
Cost of breach tree

1. Negative Social Media
   - Debilitating operational pressure

2. Negative Social Media
   - Staff lockout from system

3. Negative Social Media
   - Forensic investigation and remediation costs

4. Negative Social Media
   - Customer notification costs

5. Negative Social Media
   - Costs for contractual breach, litigation, and fines from regulators

6. Negative Social Media
   - Loss of customers and loss of sales

7. Negative Social Media
   - Staff lockout from system

8. Negative Social Media
   - Loss of customers and loss of sales

9. Loss of jobs and business failure

Costs for contractual breach, litigation, and fines from regulators
Worry tree

1. Notice the worry
2. Ask: What am I worrying about?
3. Ask: Can I do something about it?

NO
- Let worry go
- Change focus of attention

YES
- Action plan
- What? When? How?
- NOW
- LATER
- Do it!
- Schedule it
- Let worry go
- Change focus of attention

Source: Adapted from Butler and Hope 2007
Hand-in-hand with UNODC report

Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice

Cameron S. D. Brown
Australian National University, Australia

Abstract
The primary goal of this paper is to raise awareness regarding legal loopholes and enabling technologies, which facilitate acts of cyber crime. In pursuing these avenues of inquiry, the author seeks to identify systemic impediments which obstruct police investigations, prosecutions, and digital forensics interrogations. Existing academic research on this topic has tended to highlight theoretical perspectives when attempting to explain technology aided crime, rather than presenting practical insights from those actually tasked with working cyber crime cases. The author offers a grounded, pragmatic approach based on the in-depth experience gained serving with police task-forces, government agencies, private sector, and international organizations. The secondary objective of this research encourages policy makers to reevaluate strategies for combating the ubiquitous and evolving threat posed by cyber-criminality. Research in this paper has been guided by the firsthand global accounts (via the author’s core involvement in the preparation of the Comprehensive Study on Cybercrime (United Nations Office on Drugs and Crime, 2013) and is keenly focused on core issues of concern, as voiced by the international community. Further, a fictional case study is used as a vehicle to stimulate thinking and exemplify key points of reference. In this way, the author invites the reader to contemplate the reality of a cyber crime inquiry and the practical limits of the criminal justice process.
Key references

UNODC
*United Nations Comprehensive Study on Cybercrime*

Cameron S. D. Brown
*Investigating and Prosecuting Cybercrime: Forensic Dependencies and Barriers to Justice*

Cameron S. D. Brown
*Cyber-Attacks, Retaliation and Risk: Legal and Technical Implications for Nation-States and Private Entities*
*Cybersecurity Policies and Strategies for Cyberwarfare Prevention*. Advances in Digital Crime, Forensics, and Cyber Terrorism, Book Series, IGI Global, 2015 (pp. 166 – 203), DOI: 10.4018/978-1-4666-8456-0